УДК 004

**Muhammad Aamir Khan**,
MSc IT in Business innovations,
Graduate School of Economics and Management,
Ural Federal University named after the first President of Russia B. Yeltsin
e-mail: muaamirk@gmail.com
Ekaterinburg, Russia

**Hossain Ismail**,
PhD student,
Department «Nuclear Power Plants and Renewable Energy Sources»,
Ural Federal University named after the first President of Russia B. Yeltsin
e-mail: durekothau309@gmail.com
Ekaterinburg, Russia

**Maxim Medvedev**,
Associate professor,
Graduate School of Economics and Management,
Ural Federal University named after the first President of Russia B. Yeltsin
e-mail: medvedevmaa@gmail.com
Ekaterinburg, Russia

# SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

*Abstract:*
Cloud computing transforming the way of *information technology* (IT) for consuming and managing, promising improving cost efficiencies, accelerate innovations, faster time-to-market and the ability to scale applications on demand (Leighton, 2009). According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012). However, as the shape of the cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenges. In this chapter, we describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment.

*Keywords:*
Cloud Computing, Security issues, Privacy issues, Information technology, accelerate innovations.

## INTRODUCTION

According to the Wikipedia "**Cloud computing** is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand". As definition provided by the Badger et al., 2011 of National Institute for Standards and Technology (NIST), "*cloud computing* is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It is representing a paradigm shift in information technology many of us are likely to see in our lifetime. While the customers are so excited by the provided opportunities to reduce the capital costs, and the chance to divest themselves of infrastructure management and focus on core competencies, and above all the agility offered by the on-demand provisioning of computing, there are issues and challenges which need to be addressed before a ubiquitous adoption may happen.

Cloud computing is referring both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. Cloud computing had four delivery models, as outlined by Badger et al., 2011 of NIST, based on who provides the cloud services.

The business companies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services. These four delivery models are:

(i) *Private cloud environment (PCE)* in which cloud services are provided solely for an organization and are managed by the organization or a third party. PCE services may exist off-site.

(ii) *Public cloud management environment (PCME).* In this module cloud services are available to the public and owned by an organization like Microsoft, Amazon, google etc. selling the cloud services.

(iii) *Community cloud (CC) model.* As its name describe, that in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). These services may be managed by the organizations or a third party and may exist off- site. A special case of community cloud is the Government or G-Cloud. This type of cloud computing is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role).

(iv) *Hybrid Cloud Computing Model (HCC)* is a composition of different cloud computing infrastructure (public, private or community). An example for hybrid cloud is the data stored in private cloud of a travel agency that is manipulated by a program running in the public cloud.

According NIST it has identified three basic types of cloud service offerings. These models are:

I. *Software as a service* (SaaS) is used to offer renting application functionality from a service provider rather than buying, installing and running software by the user.
II. *Platform as a service* (PaaS) is used to provide a platform in the cloud, upon which applications can be developed and executed.
III. *Infrastructure as a service* (IaaS) in which the vendors offer computing power and storage space on demand.

Armbrust et al., 2009 according to hardware point of view, three aspects are new in the paradigm of cloud computing. These aspects of cloud computing are as follows:

• The illusion of infinite computing resources available on demand, thereby eliminating the need for cloud computing users to plan far ahead for provisioning.

• The elimination of an up-front commitment by cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.

• The ability to pay for use of computing resources on a short-term basis as needed and release them when the resources are not needed, thereby rewarding conservation by *letting machines and storage go when they are no longer useful.* In a nutshell, cloud computing has enabled operations of large-scale data centers which has led to significant decrease in operational costs of those data centers. On the consumer side, there are some obvious benefits provided by cloud computing. The painful reality of running IT services is the fact that in most of the times, peak demand is significantly higher than the average demand.

## ARCHICTECTURE OF CLOUD COMPUTING

In this section, we present a top-level architecture of cloud computing that depicts various cloud service delivery models. According to CSA Security Guidance, 2009 "Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of distributed services, applications, information and infrastructure comprised of pools of compute, network, information and storage resources. These components can be rapidly arranged, provisioned, implemented and decommissioned using an on- demand utility-like model of allocation and consumption. Cloud services are most often utilized in conjunction with enabling virtualization technologies to provide dynamic integration, provisioning, composition, mobility and scale.

While the other definition of cloud is suggesting the decoupling of resources from the physical affinity to and location of the infrastructure that delivers them, many descriptions of cloud go to one extreme or another by either exaggerating or artificially limiting the many attributes of cloud. This is of-

ten purposely done in an attempt to inflate or marginalize its scope. Some examples include the suggestions that for a service to be cloud-based, that the Internet must be used as a transport, a web browser must be used as an access modality or that the resources are always shared in a multi-tenant environment outside of the "perimeter." What is missing in these definitions is context.

From an architectural view is the abstracted evolution of technology, there is more confusion surrounding that how cloud of two companies are similar and different from existing models and how these similarities and differences might impact the organizational, operational and technological approaches to cloud adoption as it relates to traditional network and information security practices. There are those who say cloud is a novel sea-change and technical revolution while other suggests it is a natural evolution and coalescence of technology, economy and culture. The real truth is somewhere in between.

According to CSA Security Guidance, 2009, Cloud services are based upon five principal characteristics that demonstrate their relation to, and differences from, traditional computing approaches. These characteristics are as follows:

- **Abstraction of infrastructure:** As its name declared that the computation, network and storage infrastructure resources are abstracted from the application and information resources as a function of service delivery. Where and by what physical resource that data is processed, transmitted and stored on becomes largely opaque from the perspective of an application or services' ability to deliver it. Infrastructure resources are generally pooled in order to deliver service regardless of the tenancy model employed – shared or dedicated. This abstraction is generally provided by means of high levels of virtualization at the chipset and operating system levels or enabled at the higher levels by heavily customized file systems, operating systems or communication protocols.
- **Resource democratization:** As its name declared that the abstraction of infrastructure yields the notion of resource democratization- whether infrastructure, applications, or information – and provides the capability for pooled resources to be made available and accessible to anyone or anything authorized to utilize them using standardized methods for doing so.
- **Service-oriented architecture:** As its name declared that as the abstraction of infrastructure from application and information yields well-defined and loosely-coupled resource democratization, the notion of utilizing these components in whole or part, alone or with integration, provides a services oriented architecture where resources may be accessed and utilized in a standard way. In this model, the focus is on the delivery of service and not the management of infrastructure.
- **Elasticity/dynamism:** As its name declared that the on-demand model of cloud provisioning coupled with high levels of automation, virtualization, and ubiquitous, reliable and high-speed connectivity provides for the capability to rap-

idly expand or contract resource allocation to service definition and requirements using a self- service model that scales to as-needed capacity. Since resources are pooled, better utilization and service levels can be achieved.

- **Utility model of consumption and allocation:** As its name declared that the abstracted, democratized, service-oriented and elastic nature of cloud combined with tight automation, orchestration, provisioning and self-service then allows for dynamic allocation of resources based on any number of governing input parameters. Given the visibility at an atomic level, the consumption of resources can then be used to provide a metered utility- cost and usage model. This facilitates greater cost efficacies and scale as well as manageable and predictive costs.

**Cloud Service Delivery Models**

Three archetypal models and the derivative combinations thereof generally describe cloud service delivery. According to CSA Security Guidance, 2009 there are three individual models which are often referred to as the "SPI MODEL", where "SPI" stands for Software, Platform and Infrastructure (as a service) respectively.

- **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as web browser. In other words, in this model, a complete application is offered to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are services. On the customers' side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. In summary, in this model, the customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Currently, SaaS is used for CRM, E-Mail, Virtual Desktop, communication, games etc.

- **Platform as a Service (PaaS):** In this model, a layer of software or development environment is encapsulated and offered as a service, upon which other higher levels of service are built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. Hence, a capability is provided to the customer to deploy onto the cloud infrastructure customer-created applications using programming languages and tools supported by the provide. Although the customer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but he/she has the control over the deployed applications and possibly over the application hosting environment configurations. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of operating

systems, programming languages, database servers etc.

- **Infrastructure as a Service (IaaS):** This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers etc.).

To understanding the relationship and dependencies between these models describe that IaaS is the foundation of all cloud services with PaaS building upon IaaS, and SaaS-in turn – building upon PaaS. An architecture of cloud layer model is depicted in Figure 1.

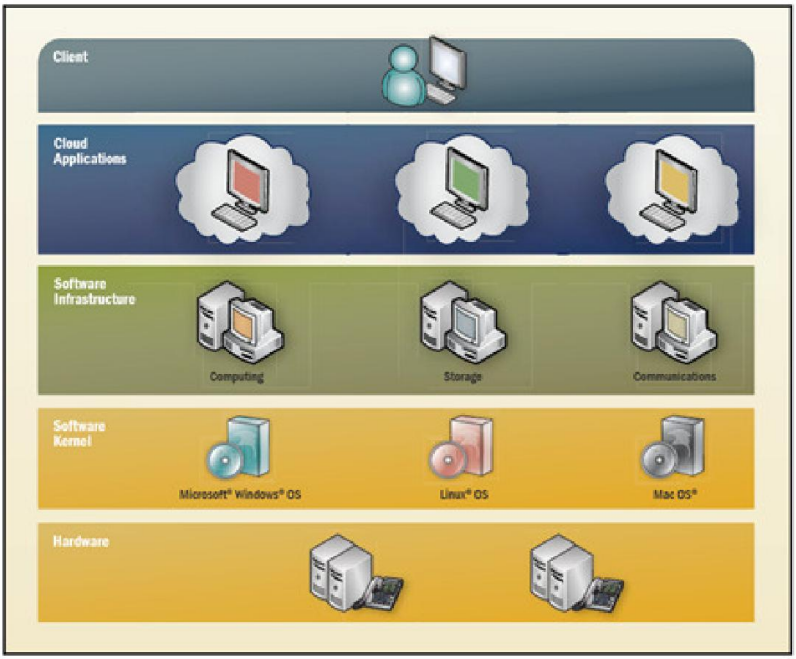


*Figure 1: An architecture of the layer model of cloud computing*

**Cloud Service Deployment and Consumption Models**

According to CSA Security Guidance, 2009 the delivery model utilization (SaaS, PaaS, IaaS), it has four primary ways in which cloud services are deployed. In which Cloud integrators can play a vital role in determining the right cloud path for a specific organization.

- **Public cloud:** As its name describe that Public clouds are provided by a designated service provider and may offer either a single- tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off- premises). All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.
- **Private cloud**: As its name describe that Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds: (i) on premise private clouds and (ii) externally hosted private clouds. The on premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider
- **Hybrid cloud:** As its name describe that Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.
- **Managed cloud:** Managed clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the

accountability/utility model of cloud. The physical infrastructure is owned by and/or physically located in the organizations' data centers with an extension of management and security control planes controlled by the designated service provider.

*Table 1*

Summary of the various features of cloud deployment models

| Deployment Model | Managed By | Infrastructure Owned By | Infrastructure Located At | Accessible and Consumed By |
|---|---|---|---|---|
| Public | It is provided by third party. | Third party provider | Off-premise | We cannot trust. |
| Private | Provided by Organization | Organization | On-premise Off-premise | Trusted |
| | Third party provider | Third party provider | On-premise Off-premise | |
| Managed | Third party provider | Third party provider | On-premise | It can be Trusted or Untrusted |
| Hybrid | Provided by organization and third party | Both organization and third party provider | Both on-premise and off-premise | It can be Trusted or Untrusted |

In addition, it is important to understand various tradeoffs between the various cloud service models:

• Generally, SaaS provides a large amount of integrated features built directly into the offering with the least amount of extensibility and in general a high level of security (or at least a responsibility for security on the part of the service provider).

• PaaS offers less integrated features since it is designed to enable developers to build their own applications on top of the platform, and it is, therefore, more extensible than SaaS by nature. However, this extensibility features tradeoffs on security features and capabilities.

• IaaS provides few, if any, application-like features, and provides for enormous extensibility but generally less security capabilities and functionalities beyond protecting the infrastructure itself, since it expects operating systems, applications and contents to be managed and secured by the customers.

## CLOUD COMPUTING SECURITY AND PRIVACY ISSUES

This section addresses the core theme of the above discussed, i.e., the security and privacy-related challenges in cloud computing. There are many security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, the virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Finally, data mining techniques may be applicable for malware detection in the clouds – an approach which is usually adopted in *intrusion detection systems* (IDSs) (Sen & Sengupta, 2005; Sen et al., 2006b; Sen et al., 2008; Sen, 2010a; Sen, 2010b; Sen 2010c).

According to Trusted Computing Group's White Paper, 2010 there are six specific areas of the cloud computing environment where equipment and software require substantial security attention. These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication of users/applications/ processes, (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response.

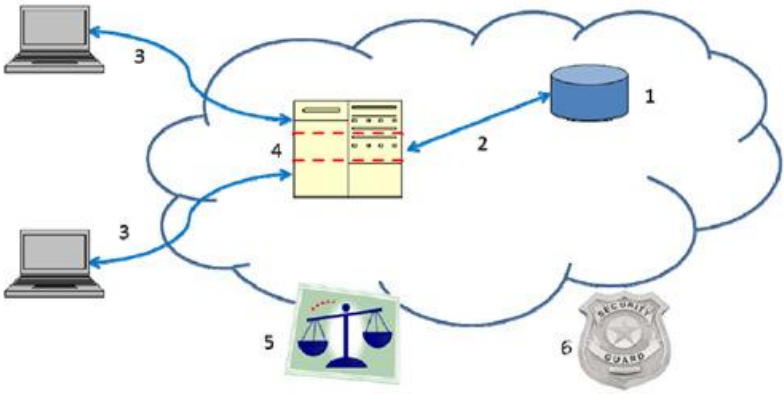


*Figure 2: Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, 3) authentication, (4) separation between customers, (5) cloud legal and regulatory issues and (6) incident response*

**Threat Vectors- What to Worry About in Security**

The landscape of threats to security and privacy change as organizations shift to cloud-based systems, storage and applications, New vectors introduced, and old ones can be demoralized in new ways.

Before categorization of new threats, it is important to acknowledge that the structure of many cloud architectures can mitigate or negate some current security threats. If data are kept in the cloud, for example, then a lost or stolen laptop is much less likely to put sensitive information at risk. According to ENISA, 2009 Standardized interfaces could make security management easier, while the scale of a provider hosting many parties can generate more information for better threat monitoring. Centralized security management and monitoring can be more effective than local efforts by IT professionals with limited security experience.

Still, moving critical systems and data to a network-accessible framework introduces new classes of vulnerabilities in and of itself, by creating new surfaces to attack and new interfaces to exploit. When those network resources are built on systems, platforms and applications shared with others, another set of threat vectors is introduced. The control mechanisms itself can be attacked, breaking down isolation between users, potentially allowing another user to access data or resources. According to Ristenpart et al.2009, even without direct access, a providers' other clients can learn valuable transaction data about an organization. According to Molnar & Schechter, 2010 the shared architecture also puts a cloud user at risk from other cloud users if their bad behavior draws attention from either law enforcement or media, leading to hardware seizure or bad publicity.

Some threat vectors are not new to cloud, but have somewhat different dynamics. In classic IT architecture, PCs inside the organization may be at risk of compromise through a host of attack vectors exploiting local applications such as browses or documents viewers. According to Zetter, 2010 If less data is stored locally, less is immediately at risk, but now the attacker could compromise credentials to gain access to the user's cloud privileges. A compromise to an entire Gmail database probably began with a compromised PC. According to Lowensohn & McCarthy, 2009 Similarly, in an attack on the Twitter management team in 2009, a compromised email password led to exposure of a wide range of other important documents in other cloud infrastructures. Shared authentication tokens can lead to brittle defenses.

Organizations must be careful to safeguard data as they move it around their o rganization, even without the benefit of cloud computing. According to Garfinkel & Shelat, 2003 When they no longer need data, it must be properly deleted, or else risk leaking sensitive data to the outside. When relying on a cloud service to handle data, appropriate care must be made to arrange for appropriate security management practices, such as encryption and appropriate deletion.

Similarly, all organizations are vulnerable to an insider attack from a trusted insider, but moving things to the cloud can raise the costs of misplaced trust. A cloud system with a well-thought out identity interface and a clear access control system can restrict access and foster accountability. However according to Sinclair & Smith, 2008, a unified data system with more people accessing more different types of data through more applications can actually make it harder to appropriately limit access and detect misuse.

**Security Issues in Cloud Computing**

Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements. But since there is no common cloud computing security standard, there are additional challenges associated with this. According to CPNI Security Briefing, 2010 many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits. In a vendor cloud model, it is ultimately down to adopting customer organizations to ensure that security in the cloud meets their own security polices through requirements gathering provider risk assessments, due diligence, and assurance activities.

Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises. The same internal and external threats are present and require risk mitigation or risk acceptance. In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing and implementing security control in a privately owned cloud. In particular, we examine the following issues:

- The treats against information assets residing in cloud computing environments.
- The types of attackers and their capability of attacking the cloud.
- The security risks associated with the cloud, and where relevant considerations of attacks and countermeasures.
- Emerging cloud security risks.
- Some example cloud security incidents.

**WORST CLOUD SECURITY THREATS**

According to www.informationweeks.com “Leading cloud security group lists the "Notorious Nine" top threats to cloud computing in 2013; most are already known but defy 100% solution”.

1. **Data Breaches**

According to the CSA report authors "Cloud computing introduces significant new avenues of attack”. The data breach at Target, resulting in the loss of personal

and credit card information of up to 110 million individuals, was one of a series of startling thefts that took place during the normal processing and storage of data. The absolute security of hypervisor operation and virtual machine operations is still to be proved. Indeed, critics question whether such absolute security can exist. The report's writers said there's lab evidence -- though none known in the wild -- that breaches via hypervisors and virtual machines may occur eventually.

2. **Data Loss**

A data breach is the result of a malicious and probably intrusive action. Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of encrypted data loses the key that unlocks it. Small amounts of data were lost for some Amazon Web Service customers as its EC2 cloud suffered "a remirroring storm" due to human operator error on Easter weekend in 2011. And a data loss could occur intentionally in the event of a malicious attack.

3. **Account Or Service Traffic Hijacking**

Account hijacking sounds too elementary to be a concern in the cloud, but CSA says it is a problem. Phishing, exploitation of software vulnerabilities such as buffer overflow attacks, and loss of passwords and credentials can all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers, and redirect customers to a competitor's site or inappropriate sites.

4. **Insecure APIs**

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these largely anonymous users might do to the service. The answer has been a public facing application programming interface, or API, that defines how a third party connects an application to the service and providing verification that the third party producing the application is who he says he is.

5. **Denial Of Service (DoS)**

Denial of service attacks are an old disrupter of online operations, but they remain a threat nevertheless. The assault by hundreds of thousands or millions of automated requests for service has to be detected and screened out before it ties up operations, but attackers have improvised increasingly sophisticated and distributed ways of conducting the assault, making it harder to detect which parts of the incoming traffic are the bad actors versus legitimate users.

6. **Malicious Insiders**

With the Edward Snowden case and NSA revelations in the headlines, malicious insiders might seem to be a common threat. If one exists inside a large cloud organization, the hazards are magnified. One tactic cloud customers should use to protect themselves is to keep their encryption keys on their own premises, not in the cloud.

7. **Abuse Of Cloud Services**

Cloud computing brings large-scale, elastic services to enterprise users and hackers alike. "It might take an attacker year to crack an encryption key using his own limited hardware. But using an array of cloud servers, he might be able to crack it in minutes," the report noted. Or hackers might use cloud servers to serve malware, launch DDoS attacks, or distribute pirated software.

8. **Insufficient Due Diligence**

"Too many enterprises jump into the cloud without understanding the full scope of the undertaking," said the report. Without an understanding of the service providers' environment and protections, customers don't know what to expect in the way of incident response, encryption use, and security monitoring. Not knowing these factors means "organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks," wrote the authors.

9. **Shared Technology**

In a multi-tenant environment, the compromise of a single component, such as the hypervisor, "exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach," the report said. The same could be said other shared services, including CPU caches, a shared database service, or shared storage.

## CONCLUSION

Today, cloud computing is being defined and talked about across the ICT industry under different contexts and with different definitions attached to it. The core point is that cloud computing means having a server firm that can host the services for users connected to it by the network. Technology has moved in this direction because of the advancement in computing, communication and networking technologies. Fast and reliable connectivity is a must for the existence of cloud computing.

Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control is transparency in the cloud implementation – somewhat contrary to the original promise of cloud computing in which cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Because of today's perceived lack of control, larger companies are testing the waters with smaller projects and

less sensitive data. In short, the potential of the cloud is not yet being realized.

When thinking about solutions to cloud computing's adoption problem, it is important to realize that many of the issues are essentially old problems in a new setting, although they may be more acute (Chow et al., 2009). For example, corporate partnerships and offshore outsourcing involve similar trust and regulatory issues. Similarly, open source software enables IT department to quickly build and deploy applications, but at the cost of control and governance. Similarly, virtual machine attacks and web service vulnerabilities existed long before cloud computing became fashionable. Indeed, this very overlap is reason for optimism; many of these cloud computing roadblocks have long been studied and the foundations for solutions exist. For the enhancement of technology, and hence healthy growth of global economy, it is extremely important to iron out any issues that can cause road-blocks in this new paradigm of computing.

**References**


1. Alliance for Telecommunications Industry Solutions. Homepage URL: http://www.atis.org.
2. Amazon S3 Availability Event: (2008). URL: http://status.aws.amazon.com/s3-20080720.html (Accessed on November 29, 2012).
3. AOL Apologizes for Release of User Search Data (2006). URL: news.cnet.com/2010-1030_3-6102793.html. August 7, 2006.
4. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinsky, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M (2009). Above the Clouds: A Berkley View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, Department of Electrical Engineering and Computer Sciences, University of California at Berkley. February 10, 2009. Available on line at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (Accessed on: November 20, 2012)
5. Association for Retail Technology Standards (ARTS). Homepage URL: http://www.nrf-arts.org.
6. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf (Accessed on: November 20, 2012).
7. Bertion, E., Paci, F., & Ferrini, R. (2009). Privacy-Preserving Digital Identity Management for Cloud Computing. IEEE Computer Society Data Engineering Bulletin, pp. 1-4, March 2009.
8. Biggs & Vidalis (2009). Cloud Computing: The Impact on Digital Forensic Investigations. In Proceedings of the 7th International Conference for Inter-

net Technology and Secured Transactions (ICITST'09), London, UK, November, 2009, pp. 1-6,
9. Blaze, M., Kannan, S., Lee I., Sokolsky, O., Smith, J. M., Keromytis, A.D., & Lee, W. (2009). Dynamic Trust Management. IEEE Computer, Vol 42, No 2, pp. 44-52, 2009.
10. Bruening, P.J. & Treacy, B.C. (2009). Cloud Computing: Privacy, Security Challenges. Bureau of National Affairs, 2009.
11. Center for the Protection of Natural Infrastructure (CPNI)'s Information Security Briefing on Cloud Computing, 01/2010, March 2010. Available Online at: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf (Accessed on: November 29, 2012).
12. Chen, Y., Paxson, V., & Katz, R.H. (2010). What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, 2010. Available Online at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html (Accessed on: November 29, 2012).
13. Chor, B., Kushilevitz, E., Goldreich, O., & Sudan, M. (1998). Private Information Retrieval. Journal of ACM (JACM), Vol 45, No 9, pp. 965-981, November 1998.
14. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In Proceedings of the ACM Workshop on Cloud Computing Security (CCSW'09), Chicago, Illinois, USA, November, 2009, pp 85-90, ACM Press, New York, USA.
15. Cloud Security Alliance. Home page URL: https://cloudsecurityalliance.org.
16. Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). CSA, April 2009. Available Online at: https://cloudsecurityalliance.org/csaguide.pdf (Accessed on: November 29, 2012).
17. Cryptographic Key Management Project Website: URL: http://csrc.nist.gov/groups/ST/key_mgmt/ (Accessed on: November 29, 2012).
18. Distributed Management Task Force. Homepage URL: http://www.dmtf.org.
19. Don't Cloud Your Vision. URL: http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63-0000779fd18c.html?nclick_check=1. (Accessed on: November 29, 2012).
20. European Network and Information Security Agency (ENISA) (2009). Cloud Computing: Cloud Computing: Benefits, Risks and recommendations for Information Security. Report No: 2009.
21. European Telecommunication Standards Institute. Homepage URL: http://www.etsi.org.

22. Extended Gmail Outage Hits Apps Admins. (2008). URL:http://www.computerworld.com/s/article/9117322/Extended_Gmail_outage_hits_Apps_admins. October 16, 2008. (Accessed on: November 20, 2012)
23. Facebook Users Suffer Viral Surge. (2009). URL: http://news.bbc.co.uk/2/hi/technology/7918839.stm. March 2, 2009. (Accessed on: November 20, 2012).
24. Flexiscale Suffers 18-Hour Outage. (2008). URL: http://www.thewhir.com/web-hosting-news/flexiscale- suffers-18-hour-outage. October, 2008. (Accessed on: November 20, 2012).
25. FTC Questions Cloud Computing Security (2009). URL: http://news.cnet.com/8301-13578_3-10198577-38.html?part=rss&subj=news&tag=2547-1_3-0-20. (Accessed on: November 29, 2012).
26. Gajek, S., Jensen, M., Liao, L., & Schwenk, J. (2009). Analysis of Signature Wrapping Attacks and Countermeasures. In Proceedings of the IEEE International Conference on Web Services, Los Angeles, California, USA, July 2009, pp. 575-582.
27. Garfinkel, S. & Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices.
28. IEEE Security and Privacy, Vol 1, No 1, pp. 17-27, January-February 2003.
29. Gartner Hype-Cycle 2012 – Cloud Computing and Big Data (2012). Available at: http://www.gartner.com/technology/research/hype-cycles/
30. Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09), pp. 169-178, Bethesda, Maryland, USA, May-June, 2009.
31. Gruschka, N. & Iacono, L. L. (2009). Vulnerable Cloud: SOAP Message Security Validation Revisited. In Proceedings of IEEE International Conference on Web Services (ICWS'09), Los Angeles, California, USA, July 2009, pp. 625-631.
32. IBM Blue Cloud Initiative Advances Enterprise Cloud Computing. URL: http://www-03.ibm.com/press/us/en/pressrelease/26642.wss. (Accessed on: November 20, 2012).
33. Institute of Electrical and Electronics Engineers (IEEE). Homepage URL: http://www.ieee.org. International Telecommunication Union – Telecommunication Standardization Sector (ITU-T). Homepage URL: http://www.itu.int/ITU-T.
34. Internet Engineering Task Force. Homepage URL: http://www.ietf.org.
35. Joshi, J.B.D., Bhatti, R., Bertino, E., & Ghafoor, A. (2004). Access Control Language for Multi-domain

36. Environments. IEEE Internet Computing, Vol 8, No 6, pp. 40-50, November 2004.
37. Ko, M., Ahn, G.-J., & Shehab, M. (2009). Privacy-Enhanced User-Centric Identity Management. In
38. Proceedings of IEEE International Conference on Communications, Dresden, Germany, June 2009, pp. 998-1002.
39. Latest Cloud Storage Hiccups Prompts Data Security Questions. URL:http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130682&source=NLT_PM. (Accessed on: November 29, 2012)
40. Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time? IEEE Computer, Vol 42, No 1, pp. 15-20, January 2009.
41. Leighon, T. (2009). Akamai and Cloud Computing: A Perspective from the Edge of the Cloud. White Paper. Akamai Technologies. Available online at: http://www.essextec.com/assets/cloud/akamai/cloud- computing-perspective-wp.pdf. (Accessed on: November 20, 2012).
42. Lithuania Weathers Cyber Attack, Braces for Round 2. URL: http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html. (Accessed on: November 20, 2012).
43. Loss of Customer Data Spurs Closure of Online Storage Service The Linkup'. URL:http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1. (Accessed on: November 20, 2012).
44. Lowensohn, J. & McCarthy, C. (2009). Lessons from Twitter's Security Breach. Available online at: http://news.cnet.com/8301-17939_109-10287558-2.html (Accessed on: November 29, 2012).
45. Microsoft Security Bulletin MS07-049. Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (937986). URL: http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx. (November 13, 2007) (Accessed on November 20, 2012).
46. Molnar, D. & Schechter, S. (2010). Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In Proceedings of the Workshop on the Economics of Information Security, 2010, Harvard University, USA, June 2010. Available online at: http://weis2010.econinfosec.org/ papers/session5/ weis2010_schechter.pdf (Accessed on: November 29, 2012).
47. Netflix Prize. URL: http://www.netflixprize.com/
48. Object Management Group. Homepage URL: http://www.omg.org. Open Cloud Computing Interface. Homepage URL: http://occi-wg.org. Open Cloud Consortium. Homepage URL: http://opencloudconsortium.org.
49. Organization for the Advancement of Structured Information Standards. Homepage URL: http://www.oasis-open.org.
50. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off Of My Cloud: Exploring Information Leakage in Third-Party

Compute Clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09), November, 2009, Chicago, Illinois, USA, pp. 199-212. ACM Press, New York, USA, 2009.
51. Salesforce.com Warns Customers of Phishing Scam. (2007) URL: http://www.pcworld.com/businesscenter/article/139353/article.html. November, 2007 (Accessed on: November 20, 2012).
52. Security Evaluation of Grid Environments. Available online at: http://www.slideworld.com/slideshows.aspx/Security-Evaluation-of-Grid-Environments-ppt-217556. (Accessed on: November 29, 2012)
53. Security Tracker. VMWare Shared Folder Bug Lets Local Users on the Guest OS Gain Elevated Privileges on the Host OS. Security Tracker ID: 1019493. URL: http://securitytracker.com/id/1019493 (Accessed on: November 20, 2012)
54. Sen, J. (2011a). A Robust Mechanism for Defending Distributed Denial of Service Attacks on Web Servers. International Journal of Network Security and its Applications, Vol 3, No 2, pp. 162-179, March 2011.
55. Sen, J. (2011b). A Novel Mechanism for Detection of Distributed Denial of Service Attacks. In Proceedings of the 1st International Conference on Computer Science and Information Technology (CCSIT'11), pp. 247-257, Springer CICS Vol 133, Part III, January 2011, Bangalore, India.
56. Sen, J. (2010a). An Agent-Based Intrusion Detection System for Local Area Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol 2, No 2, pp. 128-140, August 2010.
57. Sen, J. (2010b). An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks. In Proceedings of the 2nd IEEE International Conference on Intelligence in Communication Systems and Networks (CICSyN'10), pp. 202-207, July, 2010, Liverpool, UK.
58. Sen, J. (2010c). A Robust and Fault-Tolerant Distributed Intrusion Detection System. In Proceedings of the 1st International Conference on Parallel, Distributed and Grid Computing (PDGC'10), pp. 123-128, October 2010, Waknaghat, India.
59. Sen, J. (2010d). A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes in a Mobile Ad Hoc Network. International Journal of Network Security and its Applications (IJNSA), Vol 2, N0 4, pp. 92-104, October 2010.
60. Sen, J. (2010e). A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks. In Proceedings of the 1st International Workshop on Trust Management in Peer-to-Peer Systems (IWTMP2PS), pp. 538-547, July 2010, Chennai, India, Springer CCIS Vol 89.
61. Sen, J. (2010f). A Trust-Based Robust and Efficient Searching Scheme for Peer-to-Peer Networks. In Proceedings of the 12th International Confer-

ence on Information and Communication Security (ICICS), pp. 77-91, December 2010, Barcelona, Spain, Springer LNCS Vol 6476.
62. Sen, J. (2010g). Reputation- and Trust-Based Systems for Wireless Self-Organizing Networks. Book Chapter in Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, pp. 91-122, Al-Shakib Khan Pathan et al. (eds.), Aurbach Publications, CRC Press, USA, December 2010.
63. Sen, J. (2011c). A Secure and Efficient Searching for Trusted Nodes in Peer-to-Peer Network. In Proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems (CISIS'11), pp. 101-109, Springer LNCS Vol 6694, June 2011.
64. Sen, J. & Sengupta, I. (2005). Autonomous Agent-Based Distributed Fault-Tolerant Intrusion Detection System. In Proceedings of the second International Conference on Distributed Computing and Internet Technology (ICDCIT'05), pp. 125-131, December 2005, Bhubaneswar, India. Springer LNCS Vol 3186.
65. Sen, J., Sengupta, I., & Chowdhury, P. R. (2006a). A Mechanism for Detection and Prevention of Distributed Denial of Service Attacks. In Proceedings of the 8th International Conference on Distributed Computing and Networking (ICDCN'06), pp. 139-144, Springer LNCS Vol 4308, December 2006, Guwahati, India.
66. Sen, J., Sengupta, I., & Chowdhury, P.R. (2006b). An Architecture of a Distributed Intrusion Detection System Using Cooperating Agents. In Proceedings of the International Conference on Computing and Informatics (ICOCI'06), pp. 1-6, June, 2006, Kuala Lumpur, Malaysia.
67. Sen, J., Chowdhury, P. R., & Sengupta, I. (2006c). A Distributed Trust Mechanism for Mobile Ad Hoc Networks. In Proceedings of the International Symposium on Ad Hoc and Ubiquitous Computing (ISAHUC'06), pp. 62-67, December, 2006, Surathkal, Mangalore, India.
68. Sen, J., Chowdhury, P. R., & Sengupta, I. (2007). A Distributed Trust Establishment Scheme for Mobile Ad Hoc Networks. In Proceedings of the International Conference on Computation: Theory and Applications (ICCTA'07), pp. 51-57, March 2007, Kolkata, India.
69. Sen, J., Ukil, A., Bera, D., & Pal, A. (2008). A Distributed Intrusion Detection System for Wireless AdHoc Networks. In Proceedings of the 16th IEEE International Conference on Networking (ICON'08), pp.1-5, December 2005, New Delhi, India.
70. Sinclair, S. & Smith, S. W. (2008). Preventive Directions for Insider Threat Mitigation Using Access Control. Book Chapter No 11, S. Stolfo, S. M. Bellovin, S. Hershkop, A. D. Keromytis, S. Sinclair, & W. Smith eds. Insider Attack and Cyber Security: Beyond the Hacker. Springer, April 2008.
71. Shacham, H. & Waters, B. (2008). Compact Proofs of Retrievability. In Proceedings of the 14th International Conference on the Theory and Appli-

cation of Cryptology and Information Security: (ASIACRYPT'08), Melbourne, Australia, December 7-11, 2008. Lecture Notes in Computer Science (LNCS), Vol 5350, pp. 90-107, Springer-Verlag, Berlin, Heidelberg, Germany, 2008.
72. Shin, D. & Ahn, G.-J. (2005). Role-Based Privilege and Trust Management. Computer Systems Science and Engineering Journal, Vol 20, No 6, pp. 401-410, November 2005.
73. Song, D., Wagner, D., & Perrig, A. (2000). Practical Techniques for Searches on Encrypted Data. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, California, USA, pp. 44-55, May 2000.
74. Storage Networking Industry Association. Homepage URL: http://www.snia.org.
75. Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy, Vol 8, No 6, pp. 24-31, November-December 2010.
76. TM Forum. Homepage URL: http://www.tmforum.org.
77. Trusted Computing Group (TCG)'s White Paper (2010). Cloud Computing and Security- A Natural Match. Available online at: http://www.trustedcomputinggroup.org (Accessed on; November 2012).
78. Xen Vulnerability. URL: http://secunia.com/advisories/26986/. (Accessed on: November 20, 2012).
79. Zetter, K. (2010). Google hackers Targeted Source Code of More Than 30 Companies. Wired Threat Level. January 13 2010. Available online at: http://www.wired.com/threatlevel/2010/01/google-hack- attack/ (Accessed on: November 29, 2012).
80. Zhang, Y. & Joshi, J. (2009). Access Control and Trust Management for Emerging Multidomain Environments. Annals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyay and R.O. Rao (eds.), Emerald Group Publishing, pp. 421-452, 2009.
81. http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085?page_number=2